

AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20)

☐ Original ☐ Duplicate**FILED**  
CLERK, U.S. DISTRICT COURT

Original

**UNITED STATES DISTRICT COURT**

8/30/2023

CENTRAL DISTRICT OF CALIFORNIA

BY: \_\_\_\_\_ jm \_\_\_\_\_ DEPUTY

for the

Central District of California

United States of America

v.

SUKRU TEMUCIN ASLAN,

Defendant.

Case No. 2:23-mj-04455 -DUTY

**CRIMINAL COMPLAINT BY TELEPHONE  
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about August 30, 2023, in the county of Los Angeles in the Central District of California, the defendant violated:

*Code Section*

18 USC 1956(a)(3)(B)

*Offense Description*

Laundering Property Represented to be Proceeds of Unlawful Activity

This criminal complaint is based on these facts:

*Please see attached affidavit.*☒ Continued on the attached sheet.

/s/ Adam J. Cirillo

Complainant's signature

Adam J. Cirillo, DEA Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 8/30/2023

City and state: Los Angeles, California

A handwritten signature in black ink, appearing to read "Michael R. Wilner".

Judge's signature

Hon. Michael R. Wilner

Printed name and title

**AFFIDAVIT**

I, Adam J. Cirillo, being duly sworn, declare and state as follows:

**I. PURPOSE OF AFFIDAVIT**

1. This affidavit is made in support of a criminal complaint and arrest warrant against Sukru Temucin ASLAN ("ASLAN") for Laundering Property Represented to be Proceeds of Unlawful Activity, in violation of 18 U.S.C. 1956(a)(3)(B), on or about July 6, 2023.

2. This affidavit is also made in support of applications for warrants to search the following:

a. 2590 Redhill Avenue Unit 5167, Santa Ana, CA 92705 (the "SUBJECT PREMISES"), as described more fully in Attachment A-1; and

b. The person of ASLAN, as described more fully in Attachment A-2.

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations 18 U.S.C. 1956 (laundering of monetary instruments) (the "Subject Offense"), as described more fully in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant, and does not purport to set forth

all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## **II. BACKGROUND OF AFFIANT**

5. I am a Special Agent with the United States Department of Justice, Drug Enforcement Administration ("DEA"). I am currently assigned to the Los Angeles Field Division ("LAFD"). At the LAFD, I am assigned to the Financial Investigations Group ("FIG"). As such, I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7); that is, an officer of the United States empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

6. I have worked for the DEA as a Special Agent since December 2019. Prior to becoming a DEA Special Agent, I was a sworn law enforcement officer with the Cobb County Police Department in the state of Georgia. As such, I was tasked with conducting law enforcement operations involving drug nexuses. Cumulatively, I have approximately six years of sworn law enforcement experience.

7. I have received training and have experience investigating violations of both state and federal narcotics and money laundering laws, including, but not limited to 21 U.S.C. §§ 841, 846, 952, 959, and 963, and 18 U.S.C. § 1956(a). I have been involved in electronic surveillance methods, the debriefing of defendants, informants, and witnesses, as well as others who

have knowledge of the manufacturing, distribution, transportation, and storage of controlled substances and the laundering of drug proceeds. Prior to becoming a DEA Special Agent, I attended a 17-week Basic Agent Academy at the DEA Training Academy in Quantico, Virginia. I also attended a 23-week police academy in Cobb County, Georgia. Over the course of my career, I have received both formal and informal training regarding money laundering, drug trafficking and distribution, and other applicable criminal laws.

8. Throughout my law enforcement career, I have investigated individuals and criminal organizations, which have represented a significant threat to public safety. Specifically, during the course of my employment, I have received comprehensive, formalized instruction to include such topics as drug identification, money laundering techniques, patterns of drug trafficking, complex conspiracies, the exploitation of narcotics traffickers' telecommunications devices, criminal law, surveillance, and other investigative techniques. I have participated in investigations into the unlawful possession with intent to distribute, and distribution of narcotics and controlled substances, the laundering of narcotics proceeds, trafficking of controlled substances and list (precursor) chemicals, and conspiracies associated with those offenses.

9. I have participated in many aspects of drug investigations. I am familiar with narcotics traffickers' methods of operation, including the manufacturing, storage,

transportation, and distribution of narcotics, the collection of money that represents the proceeds of narcotics trafficking, and money laundering. I am also familiar with the manner in which narcotics traffickers transport and distribute narcotics in areas they control.

10. In conducting major narcotics investigations, I have become aware of many techniques utilized by narcotics traffickers. I have learned that these individuals utilize various tactics to avoid detection and/or apprehension by law enforcement officials. Techniques used by members of these organizations include the use of multiple locations, utilizations of numerous co-conspirators, the use of pagers, pay telephones, cellular telephones, and the use of hidden compartments in vehicles.

### **III. SUMMARY OF PROBABLE CAUSE**

11. Since November 2022, LA DEA agents have been conducting an undercover operation focused on a Los Angeles-based money launderer, Sukru Temucin ASLAN. In a series of two controlled transactions, on July 6, 2023 and August 23, 2023, confidential informants working at the direction of DEA agents, negotiated to drop off U.S. currency to ASLAN and have ASLAN wire transfer the money (less a commission) to a foreign bank account. Before the transactions, a confidential informant told ASLAN that the U.S. currency being provided to ASLAN was proceeds from the sale of illegal narcotics. For example, a confidential source specifically told ASLAN that the confidential source was involved in a drug trafficking

organization that trafficked methamphetamine, cocaine, and fentanyl. As discussed below, at various times ASLAN requested that the confidential source sell ASLAN large quantities of cocaine.

12. ASLAN drove to the August 23, 2023, transaction in a white 2022 Tesla Model X bearing California license plate number CD49 J02 which was used to transport the purported illicit proceeds and travel to banks to conduct the subsequent wire transfer. Additionally, the SUBJECT PREMISES is ASLAN's residence and is linked to the Wells Fargo account that ASLAN used to conduct the money laundering transaction on July 6, 2023.

#### **IV. STATEMENT OF PROBABLE CAUSE**

13. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

##### **A. A DEA Source Identifies ASLAN as a Potential Money Launderer**

14. In July 2020, a DEA Nicosia Country Office (NCO) Confidential Source<sup>1</sup> (CS-1) identified ASLAN as an individual who could launder drug proceeds.

15. Based on my review of reports and speaking to other law enforcement officers, I know that in November 2022, CS-1

---

<sup>1</sup> CS-1 has worked with the DEA in multiple prior investigations. CS-1 is being paid to assist law enforcement. I have personally met with CS-1. I and other law enforcement have taken steps to corroborate the information provided by CS-1. The information CS-1 has provided has been reliable and accurate.

obtained ASLAN's telephone, which was 310-420-0240 (hereinafter "Subject Telephone 1"). Under the direction of DEA agents, CS-1 called ASLAN to discuss his money laundering services. During the conversation, ASLAN expressed an interest in laundering money but wanted to discuss the details in person. CS-1 and ASLAN agreed to meet in early 2023 in Los Angeles to discuss the details.

**B. CS-1 Meets with ASLAN to Discuss ASLAN's Money Laundering Services in Early 2023**

16. DEA NCO agents contacted Los Angeles Field Division (LAFD), Financial Investigations Group (FIG) to provide details pertaining to ASLAN. Specifically, agents received subpoena returns related to Chase Bank accounts associated with ASLAN. On at least one document with ASLAN's identifying information, Subject Telephone 1 was included as his contact number.

17. From a variety of law enforcement and open source databases, agents were able to identify ASLAN, his addresses, associated businesses, bank accounts, vehicles, and also obtained a California DMV photograph of ASLAN. ASLAN's Wells Fargo bank account, which is in his own name, lists the SUBJECT PREMISES as ASLAN's address.

18. Based on my review of law enforcement reports and recordings, on March 7, 2023, CS-1 and ASLAN met in West Hollywood, California. During the meeting, which was recorded, CS-1 explained to ASLAN that he/she works with a Mexican group in the Los Angeles area that was involved in drug trafficking. According to CS-1 from a subsequent debriefing, ASLAN asked what

type of drugs the organization trafficked, to which CS-1 specified methamphetamine, cocaine, and fentanyl. At that time, CS-1 told ASLAN that CS-1 was interested in ASLAN's money moving services. At the conclusion of the meeting, ASLAN agreed to meet CS-1's associate the following day to discuss details.

**C. ASLAN Meets CS-2 And Offers His Money Laundering Services**

19. Based on my review of law enforcement reports and recordings, I know that on March 8, 2023, CS-1 and ASLAN met in Burbank, California. Also present was a Los Angeles based confidential source ("CS-2"),<sup>2</sup> who was introduced to ASLAN as the associate of CS-1. During the meeting, ASLAN told CS-2 that he could start by taking \$50,000 in cash and transferring it to wherever CS-2 needed the money. ASLAN stated that eventually he could move up to \$10,000,000 each month. ASLAN then provided CS-2 commission rates for moving funds to different countries. At the conclusion of the meeting, ASLAN obtained CS-2's telephone number. ASLAN also asked CS-2 to download the Signal encrypted messaging application so that they could communicate in a secure fashion.

---

<sup>2</sup> CS-2 began working for DEA in 2021. In or around September 2021, the CS was arrested for possession of methamphetamine. The CS is currently providing information to investigators for monetary compensation. The CS has provided truthful information to investigators which has been independently corroborated. The CS has previously provided information to the DEA in another investigation that has been corroborated and proven to be reliable, and has not provided any information that was later determined to be false or otherwise unreliable.



20. On March 30, 2023, ASLAN sent a text message<sup>3</sup> through the Signal messaging application to CS-1 and told CS-1 to let CS-2 know that ASLAN could do bank wire transfers for 5 percent to any country.

**D. On July 6, 2023, ASLAN and CS-2 Coordinate the First Transfer of Funds to Austria**

21. On June 22, 2023, CS-2 acting at the direction of DEA agents, placed a recorded phone call to ASLAN at Subject Telephone 1. During the conversation, and using coded language, CS-2 asked ASLAN if ASLAN could send \$35,000 to Austria for a five percent fee. ASLAN responded that he could.

22. On June 23, 2023, using Subject Telephone 1, ASLAN sent CS-2 a recorded text message stating that ASLAN could move the funds to Austria for a \$2,000 commission fee.

23. On July 5, 2023, CS-2 acting at the direction of DEA agents, sent a recorded text message to ASLAN at Subject Telephone 1 and asked if ASLAN was available to meet the following day. CS-2 told ASLAN that CS-2 was going to send his/her associate ("CS-3") to meet ASLAN.

24. On July 6, 2023, through a series of additional recorded text messages and phone calls, ASLAN agreed to meet CS-3<sup>4</sup> at a Home Depot in Santa Ana, California. CS-2 sent ASLAN a

---

<sup>3</sup> All text messages and calls between CS-1, CS-2, CS-3, and ASLAN have been preserved and I have reviewed them in preparing this affidavit.

<sup>4</sup> CS-3 has worked with the DEA in multiple prior investigations. CS-3 was previously involved in drug trafficking and was charged. CS-3 is receiving immigration benefits and is being paid to assist law enforcement. I have personally met with CS-3. I and other law enforcement have  
(footnote cont'd on next page)

recorded text message with a bank account number for an account located in Austria to deposit the funds into. This account was controlled by law enforcement.

25. DEA agents, including myself, set up surveillance at the Santa Ana Home Depot. DEA agents then saw ASLAN arrive at the Home Depot in a black Range Rover bearing California license plate 7PTL458. During surveillance, I saw that ASLAN was the only occupant inside the Range Rover and that ASLAN parked directly next to CS-3. I subsequently observed CS-3 provide \$35,000 in purported drug proceeds to ASLAN, which was concealed inside a plastic white and blue AT&T shopping bag.

26. After the exchange, agents then followed ASLAN to a Wells Fargo bank located at 2677 Park Ave., in Tustin, California. Agents then saw ASLAN walk into Wells Fargo carrying the same blue and white AT&T bag that CS-3 had given to him at the Home Depot. Shortly thereafter, ASLAN sent CS-2 a photograph of a bank wire confirmation showing that \$33,000 had been sent to an Austrian bank account. I reviewed bank records from Wells Fargo, which confirmed that ASLAN deposited \$35,000 into his bank account on July 6, 2023, and then sent out \$33,000 via wire transfer. Law enforcement officials in Austria confirmed that on July 10, 2023, €30,148 was received in the undercover account that ASLAN had been instructed to wire the funds into.

---

taken steps to corroborate information provided by CS-3 and the information by CS-3 has shown to be reliable and accurate.

**E. ASLAN Using Code Language Requests To Purchase Illegal Narcotics From CS-2**

27. Based on law enforcement reports and my knowledge of the investigation, I know that following the transfer of funds by ASLAN on July 6, 2023, ASLAN and CS-2 exchanged recorded text messages using coded language, which based on my experience and training, involved ASLAN asking to buy distribution quantities of cocaine from CS-2. As discussed below, CS-2 and ASLAN at first referred to cocaine using the term "tequilas," but subsequently discussed ASLAN purchasing illegal drugs more overtly.

28. First, on or about July 7, 2023, ASLAN in a text message asked CS-2 if he/she could bring a "gift" to ASLAN the next time the two of them met and that it was "hard to find good gifts around here." In response, CS-2 asked ASLAN if he liked "tequila." ASLAN informed CS-2 that he did like tequila and CS-2 told ASLAN that CS-2 could give him a good price for tequila. ASLAN indicated that CS-2 should let ASLAN taste the tequila and that ASLAN had big customers who were also interested in tequila. ASLAN told CS-2 that "we can sell in bulk." CS-2 then asked ASLAN how much ASLAN's customers pay for each tequila. ASLAN told CS-2 that it depended on the quality, type, and where the tequila was from. CS-2 told ASLAN that his tequila was from Colombia and to let CS-2 know if ASLAN wanted some. ASLAN said that he would want some tequila if CS-2 could arrange it.

29. Based on my knowledge, training, and experience, I determined from the recorded text messages that ASLAN and CS-2

were discussing cocaine and that ASLAN was looking to purchase cocaine from CS-2 in order to distribute it to other individuals.

30. On July 12, 2023, CS-2 and ASLAN exchanged a series of recorded text messages utilizing Subject Telephone 1. CS-2 asked ASLAN how much tequila ASLAN was looking to purchase. ASLAN stated that he would need a sample for a bulk buyer. ASLAN told CS-2 that he had four people interested in doing business with him. ASLAN stated that two of these individuals were located overseas and the other two were in other states. ASLAN also stated that he could deliver any samples of the product to the individuals who wanted to do business with him and that his only concern was the quality of the product.

31. Based on my knowledge, training, and experience, I determined from the recorded text messages that ASLAN was referring to the fact that he has at least four people that he was working with regarding cocaine distribution located both in and outside of the United States. I also understood ASLAN to be informing the CS-2 that he could transport the cocaine himself.

32. As described below, ASLAN discussed purchasing two "bricks" and haggled with CS-2 over the price of a potential kilograms quantity drug transaction.

**F. ASLAN and CS-2 Attempt to Coordinate a Second Transfer of Funds on August 23, 2023**

33. On August 14, 2023, CS-2 received a recorded phone call from telephone number 657-621-2992 ("Subject Telephone 2"). The user of the telephone identified himself as "Temo" and told

CS-2 that his other phone's battery was dead. Based on my knowledge of the investigation and reviews of past recorded calls with ASLAN, I determined that it was ASLAN who called from Subject Telephone 2.

34. Additionally, subscriber information from T-Mobile for Subject Telephone 2, shows the subscriber is Digitruckz LLC. Through the issuance of subpoenas, I know that Digitruckz LLC maintains a US Bank account and that ASLAN is the only authorized signatory on the account.

35. During the conversation, in coded language, ASLAN asked CS-2 to let ASLAN know about the purchase of the tequila because one of ASLAN's "guys" could pick it up in Los Angeles. During that conversation, CS-2 asked ASLAN about moving \$75,000 into the Austrian account. ASLAN agreed and suggested meeting on Wednesday the 16<sup>th</sup> to transfer the funds. ASLAN agreed to charge \$2,000 as a commission for moving the funds. ASLAN joked that the fee was going to be \$2,000 plus his "gift" before laughing and saying he was just kidding.

36. Later that day, through a separate recorded phone conversation, CS-2 acting at the direction of DEA agents, called ASLAN on Subject Telephone 2 and asked if Wednesday, August 16, 2023, would still work to pick up the cash to transfer to the Austrian account. Through the use of coded language, CS-2 informed ASLAN, on a recorded telephone call, that they could also talk about the "powder" at that meeting. ASLAN responded that he was waiting for CS-2 to give an answer on price and that his people were ready to pick up the product, but that there

were other options in the market. ASLAN said that the most important thing was to get the best price for the best quality. ASLAN stated that "two bricks" was only to test, after that each time will be "10, 20, 10, 20." CS-2 asked ASLAN if they could buy five for the first purchase. To which, ASLAN said it would depend on the price and that if CS-2 was able to give ASLAN a good price, ASLAN and his associates could buy five. CS-2 said that they could meet Wednesday and talk about it. Based on my knowledge, training, and experience, I determined that ASLAN was talking with CS-2 about purchasing multiple kilograms of cocaine.

37. On the same date but through a separate recorded phone conversation, ASLAN called CS-2 from Subject Telephone 2, where the two again spoke of the purchase of cocaine. ASLAN informed CS-2 that his people were good for five kilograms, but needed a price immediately. ASLAN and CS-2 haggled over price, before CS-2 informed ASLAN that if he got at least "8", CS-2 could do "12" each. Based on my knowledge, training, and experience, CS-2 was informing ASLAN that if he purchased at least 8 kilograms of cocaine, CS-2 would charge ASLAN \$12,000 per kilogram.

38. On August 18, 2023, ASLAN using Subject Telephone 1, sent CS-2 a recorded text message. ASLAN through the use of coded language, informed CS-2 that ASLAN and his associates were ready to purchase 8 kilograms of cocaine and asked CS-2 when he/she could arrange for delivery in Los Angeles.

39. On August 21, 2023, ASLAN called CS-2 from telephone number 424-413-4444 ("Subject Telephone 3"). From a voice

comparison with Subject Telephone 1 and Subject Telephone 2, I was able to determine that ASLAN was the caller of Subject Telephone 3. ASLAN inquired with CS-2 if he/she had read ASLAN's text message about the 8 pieces. CS-2 informed ASLAN that his/her boss said it was good and that CS-2 would let ASLAN know about meeting for the delivery.

40. Agents previously received subpoena returns from Wells Fargo for accounts that were associated to ASLAN.<sup>5</sup> From the documents that were received, I identified that Subject Telephone 3 was listed as the business phone number for SOHO CLINIC USA LLC on account opening paperwork that was signed by ASLAN on December 3, 2021. I also know from California business filings from the Secretary of State website, that ASLAN is the registered agent of SOHO CLINIC USA.

**G. ASLAN Conducts Another Financial Transaction Involving Purported Proceeds of Narcotics Sales On August 23, 2023**

41. On August 22, 2023, CS-2 sent a recorded text message to ASLAN at Subject Telephone 1 and inquired if ASLAN could meet CS-2 the following day at 11:00 am, ASLAN responded that he could. Through additional recorded text messages, ASLAN agreed to meet CS-2 in the Santa Ana, California area.

42. On August 23, 2023, CS-2, through a recorded text message to Subject Telephone 1, informed ASLAN that CS-2 was going to send his/her associate to drop off the funds because CS-2 was busy. ASLAN then inquired with CS-2 if his/her

---

<sup>5</sup> As described above in paragraph 17, these accounts were in ASLAN's own name and listed the SUBJECT PREMISES as his address.

associate was going to bring any samples and that ASLAN's connections were serious about potentially doing 20 to 30 pieces a month.

43. That same day, I instructed, an LAFD DEA agent acting in an undercover (UC) capacity to send a recorded text message to Subject Telephone 1, informing ASLAN that the UC would meet ASLAN around 12:30 pm in Santa Ana. The UC texted ASLAN to meet at a Starbucks located at 1248 E 17th St, Santa Ana, CA. At approximately 12:51 pm, DEA agents who were set up on surveillance in the parking lot of the Starbucks observed a white Tesla with a paper license plate arrive in parking lot of the Starbucks.

44. ASLAN texted the UC that he was at the location in white 2022 Tesla Model X with California license plate number CD49JO2 (the "TESLA"). The UC then walked over to the TESLA and ASLAN rolled down the passenger window. The UC then handed over a Disneyland plastic shopping bag containing \$75,000 to ASLAN.

45. Shortly after the UC provided the \$75,000 to ASLAN, CS-2 sent a recorded text message to ASLAN directing him to transfer the funds to the same UC law enforcement account located in Austria.

46. Shortly after ASLAN left the Starbucks, I located the TESLA with paper plates parked on the 5<sup>th</sup> floor of parking garage for the Broadstone Atlas apartments located at 2590 Redhill Ave, Santa Ana, California (the "SUBJECT PREMISES"). From my knowledge of the investigation, I know that ASLAN met with CS-2 in March in the TESLA. Additionally, from the issuance of



subpoenas, I know that ASLAN listed the SUBJECT PREMISES as his residence on his Wells Fargo account.

47. Shortly after locating the TESLA, I saw ASLAN departing the parking garage. Agents then followed ASLAN to a Wells Fargo located at 2677 Park Ave, Tustin, CA. Agents observed ASLAN park the Tesla in the parking lot of the Wells Fargo, exit carrying a black backpack, and walk into the Wells Fargo. A short time later, ASLAN left the Wells Fargo carrying the same black backpack and reentered the TESLA.

48. Agents then followed ASLAN from the Wells Fargo to a US Bank located at 4180 Barranca Pkwy, Irvine, CA. Agents watched ASLAN park and walk into the US Bank with the same black backpack identified earlier at Wells Fargo. Approximately 25 minutes later, agents observed ASLAN exiting the US Bank with the same black backpack that appeared to lighter and got into the TESLA.

49. Through recorded text messages between CS-2 and ASLAN, agents were able to determine that ASLAN was going to send the money tomorrow morning because it was after 2:00 pm. ASLAN also indicated that he was going to send the money from a different bank, because he did not want to send the money from the same account to the same person as the previous transaction.

50. On August 24, 2023, through a series of recorded text messages between ASLAN with Subject Telephone 1 and CS-2, ASLAN informed CS-2 that the bank wire was sent and he would be sending CS-2 the paperwork soon.

51. On or around August 25, 2023, through a series of recorded text messages between ASLAN with Subject Telephone 1 and CS-2, ASLAN sent a photograph of a bank wire transfer confirmation from US Bank. The confirmation indicated that \$72,960 was sent to the same UC Austrian account. There was a \$40.00 USD bank wire fee that was taken from the \$73,000. The remaining \$2,000 was ASLAN's commission fee previously agreed upon between CS-2 and ASLAN. The wire confirmation indicated that the money was sent from an account ending in 7319 with the name "JEXITRUCK LLC" along with the name "SE\*\*\* K\*\* OS\*\*\*\*\*". The bank wire confirmation was dated from August 24, 2023.

**V. TRAINING AND EXPERIENCE REGARDING EVIDENCE ASSOCIATED WITH THE SUBJECT OFFENSE**

52. Based upon my training and experience, as well as the collective knowledge and experience of other assisting agents, I am aware that it is a common practice for individuals who engage in unlawful monetary transactions and money laundering to keep records, proceeds from the transactions, and other evidence at their residences.

53. Based on my training, I know that records, in particular, are often maintained by money launderers. Based on my training in money laundering and drug trafficking organizations, I know that money launderers tend to keep their records for a long period of time. Money launderers, for example, must maintain records such as lists that contain information for clients, information about banks and other financial accounts the individual uses to conduct illicit

financial transactions, and other records used to facilitate the illicit financial transactions, and keep them immediately available in order to efficiently conduct their business.

54. It is also a common practice for those involved in the SUBJECT OFFENSE to conceal at their residences large sums of money, either the proceeds from unlawful money transactions or money received from exchanging cryptocurrency for cash. In order to further wash illicit proceeds, those involved in the SUBJECT OFFENSE often make use of wire transfers, cashier's checks, and money orders to pay for controlled substances. Evidence of such financial transactions and records relating to income and expenditures of money and wealth in connection with the SUBJECT OFFENSE is also often maintained in their residences.

55. From my background and experience and from speaking with other agents who investigate money laundering offense, I know that individuals engaged in illegal income producing businesses seek to conceal the income generated from such businesses. In particular, individuals engaged in money laundering often conduct their transactions in cash to avoid creating bank records related to such transactions and/or purchase expensive items such as jewelry, gold, silver to conceal the receipt of large amounts of cash. I am aware that the proceeds generated from both legal and illegal activities may be spent many years after the activity has stopped. Thus, records reflecting income and expenditures for the time period spanning the activity and those years immediately following the end of this activity are essential to any financial investigation.

56. Individuals who amass proceeds from legal or illegal activities routinely attempt to further that conduct and/or conceal the existence and source of their funds by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, cashier's checks, money drafts, traveler's checks, wire transfers, money orders, etc. I know from personal knowledge that individuals attempting to conceal income from the government often use a variety of methods to conceal the income including creating false business entities, using known and unknowing individuals, and hide assets, in order to disguise and conceal income.

57. I know from my training and experience that individuals involved in money laundering will often keep track of cash and other resources by taking photos of such items. Those photos may sometimes be taken or stored on cellular phones. Individuals involved in such illegal activities will often need to keep track of cash and other resources by photos and other personal documentary means because they do not want to deposit funds into a bank account, which would create records of such cash. I know that such photos may be found on cellular phones of such individuals.

58. Additionally, it is commonplace for persons engaged in money laundering, including those laundering drug proceeds, to access and use the darkweb to conduct and/or conceal their unlawful activity. Accessing the darkweb can occur by using a USB or flash-drive device. Based on my training and experience,

individuals who have such valuable information store this information in multiple locations, such that it is safe from theft and/or law enforcement and compartmentalized.

59. Based on my training and experience, I also know that those involved in money laundering and other unlawful monetary transactions usually keep transaction records and other evidence related to their criminal activity at their residences, inside their vehicles, and on their persons, including their digital devices. Notably, those involved in money laundering generally maintain and use numerous digital devices, and keep those devices (including backup devices in the event that a cell phone or other digital device necessary for the SUBJECT OFFENSE is seized by law enforcement) at their homes, in the vehicles, and on their persons. Specifically, I know that those involved in the SUBJECT OFFENSE generally maintain:

a. Books, records, receipts, notes, ledgers, and other papers relating to the conducting illicit currency transactions;

b. Personal books and papers reflecting names, addresses, telephone numbers, and other contact or identification data relating to customers or other participants in the SUBJECT OFFENSE, including personal property tending to show the existence and/or location of cash used to further and/or conduct the SUBJECT OFFENSE, including, but not limited to, storage locker receipts, maps, safety deposit keys and corresponding records, and money-counting machines;

c. Cash, currency, and records relating to the

SUBJECT OFFENSE and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, bank statements, passbooks, checkbooks, check registers, and prepaid debit cards;

d. Documents indicating travel in interstate and foreign commerce, such as travel itineraries, plane tickets, boarding passes, motel and hotel receipts, passports and visas, credit card receipts, and telephone bills;

e. Photographs, negatives, screenshots, video recordings, films, electronic storage devices and the contents therein, and slides related to the SUBJECT OFFENSE, including customer contact information, screenshots of text messages by and between co-conspirators and/or customers, among others;

f. Items of personal property that tend to identify the person(s) in residence, and the occupancy, control, or ownership of the subject premises, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys;

g. Devices used to communicate with other individuals involved in the SUBJECT OFFENSE, including computers, cellular telephones, digital watches and other communication and/or storage devices, phone answering machines, and devices used to conduct counter-surveillance against law enforcement, such as radio scanners, police radios, surveillance; and

h. cameras and monitors, anti-bugging devices and devices used to detect the presence of wiretaps, recording devices or transmitters, and/or receipts or literature describing the same.

#### **VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES**<sup>6</sup>

60. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

---

<sup>6</sup> As used herein, the term "digital device" includes the SUBJECT DEVICES and any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.



61. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises or in a short period of time for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

62. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or

eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress ASLAN's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of ASLAN's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

a. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person

may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located during the execution of the search: (1) depress the person's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

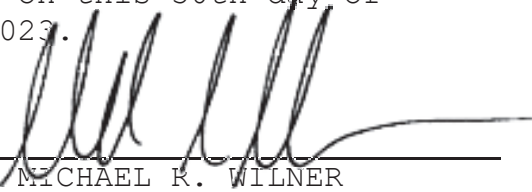
63. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

## **VII. CONCLUSION**

64. For all of the reasons described above, there is probable cause to believe that Sukru Temucin ASLAN has committed Laundering Property Represented to be Proceeds of Unlawful Activity, in violation of 18 U.S.C. 1956(a)(3)(B), on or about July 6, 2023. There is also probable cause that the items to be

seized described in Attachment B will be found in a search of the SUBJECT PREMISES described in Attachment A-1 and the person of ASLAN as described more fully in Attachment A-2.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 30th day of August, 2023.

A handwritten signature in black ink, appearing to read 'MW', is written over a horizontal line.

HONORABLE MICHAEL R. WILNER  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A-1**

PREMISES TO BE SEARCHED

The premises to be searched is located at 2590 Redhill Avenue, Unit 5167, Santa Ana, CA 92705 (the "SUBJECT PREMISES"). The SUBJECT PREMISES is an apartment within an apartment complex located at 2590 Redhill Avenue. The doorway into the SUBJECT PREMISES as depicted in the photograph below, is a grey door with "PH5167" listed on it. The search shall include any appurtenances, outbuildings, garages, sheds, carports, storage facilities, and containers -- such as storage lockers, storage spaces, or trash cans -- assigned to Unit 5167.



**ATTACHMENT A-2**

PERSON TO BE SEARCHED

The person of Sukru Temucin ASLAN ("ASLAN"), with date of birth September 15, 1985, and California Driver's License Number Y7999372. California DMV records list ASLAN as standing six feet five inches tall, with black hair and brown eyes.

The search of ASLAN shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, folders, and bags that are within ASLAN's immediate vicinity and control at the location where the search is executed. The search shall not include a strip search or a body cavity search.



**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. 1956 (laundering of monetary instruments) (the "Subject Offense"), namely:

a. Any books, records, receipts, notes, ledgers or other documents related to the acquisition, purchase, transportation, secreting and/or movement of United States and foreign currency, or other assets both, domestically and internationally;

b. Papers and other items relating to domestic and international travel, including but not limited to passports, visas, tickets, hotel bills, car rental invoices, notes, receipts or itineraries;

c. Books and records of corporations, partnerships, trusts and/or businesses, both domestic and foreign, including but not limited to: articles of incorporation or other formation or dissolution documents, bylaws, minutes of any corporate, board or shareholder's meeting, stock registers or other records identifying corporate shareholders, records reflecting the true or beneficial owner of any business, documentation evidencing the secreting, movement, transfer, or conversion of assets, both monetary and non-monetary, records identifying shareholders,

partners, directors, or officers, income or excise tax returns and/or copies, corporate seals, financial statements, journals, ledgers, notes, workpapers, real estate transaction records, bank statements and related records, brokerage account statements and related records, cancelled checks, deposit slips and other items, withdrawal slips and other items, passbooks, letters of credit, credit card statements and receipts, money orders, bank drafts and cashiers checks, bank checks, safe deposit box keys, receipts, invoices, lease agreements, correspondence, agreements, declarations, certifications, powers-of-attorney and other items evidencing the ownership or control of other business entities, and other items evidencing income, expenditures, assets, liabilities or investments;

d. Books and records of personal income, expenditures or investments, both domestic and foreign, including but not limited to: income or excise tax returns and/or copies, financial statements, journals, ledgers, notes, workpapers, bank statements and related records, cancelled checks, passbooks, letters of credit, credit card statements and receipts, money orders, bank drafts and cashiers checks, bank checks, safe deposit box keys, brokerage or other financial institution transaction statements, stocks, bonds, mortgages, real estate transaction records, receipts, invoices, and other



items evidencing income, expenditures, assets, liabilities or investments;

e. Records of loans, contracts, mortgages, notes, agreements, applications, schedules, records of payments, financing statements, collateral records, and other financial records.

f. Address and/or telephone books, appointment logs, daily or monthly planners, Rolodexes, meeting schedules, any and all papers reflecting names, addresses, telephone numbers, pager numbers, fax numbers and/or telex numbers of co-conspirators and individuals with whom a financial relationship exists, financial institutions and other individuals or businesses with whom a financial relationship exists;

g. Records relating to the use of landline, credit card, and cellular telephone services, including cellular telephones, facsimile machines and the stored electronic communications therein.

h. Indicia of occupancy, residency, rental and/or ownership of the premises described herein, including but not limited to deeds, deeds of trust, mortgage statements and payments, property tax assessments and payments, utility and telephone bills, repair and maintenance receipts, rental, purchase or lease agreements and keys;

i. Records relating to the rental of post office boxes or drop boxes, domestic and foreign;

j. All documents reflecting the names of personal aliases, corporate entities, shell corporations, partnerships, relatives and associates (nominees);

k. Any and all documentation containing telephone, credit card, and computer access codes;

l. Personnel or payroll records;

m. Any ledgers, books, records, correspondence, applications, facsimile transmissions, notes or receipts relating to expenditures to include the acquisition, conversion, movement, transfer and disbursement of monies, funds, and financial instruments;

n. Contents of any calendar or date book;

o. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

q. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

r. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

s. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

t. evidence of the attachment of other devices;

u. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

w. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

y. records of or information about Internet Protocol addresses used by the device;

z. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

aa. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

bb. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

store digital data (excluding analog tapes such as VHS); and security devices.

## **II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)**

2. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to

determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling

within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

3. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. During the execution of this search warrant, law enforcement is permitted to: (1) depress ASLAN's thumb- and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of ASLAN's face with his or her eyes open to



activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.